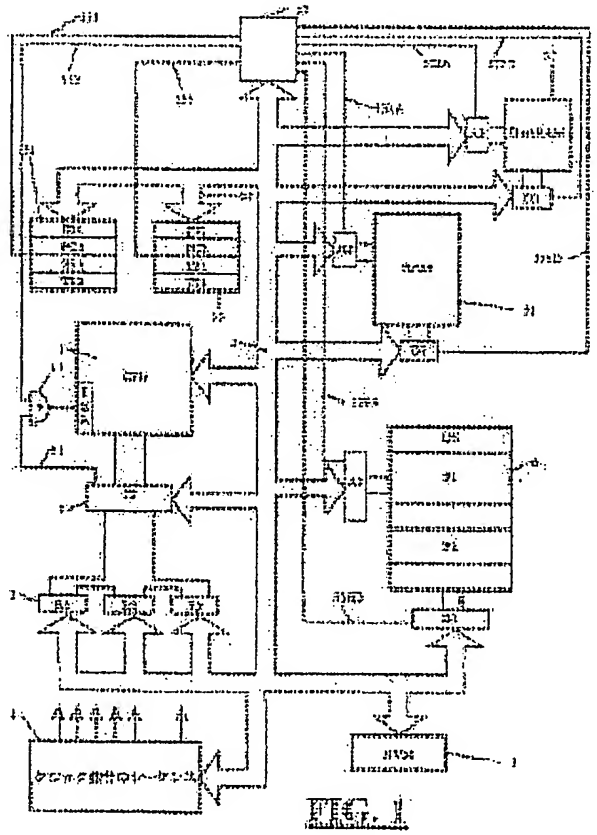
UNPREDICTABLE MICROPROCESSOR OR MICROCOMPUTER

Publication number: JP2002055883 (A)
Publication date: 2002-02-20
Inventor(s): UGON MICHEL
Applicant(s): BULL CP 8 SA
Classification:
- international: ***G06F11/22; G06F1/00; G06F9/46; G06F9/48; G06F12/14; G06F15/78; G06F21/00; G06F21/06;*** **G06F11/22; G06F1/00; G06F9/46; G06F12/14; G06F15/76; G06F21/00;** (IPC1-7): G06F12/14; G06F15/78
- European: G06F21/00N3P; G06F9/46G; G06F9/48C4; G06F21/00N3J5; G06F21/00N3J5D
Application number: JP20010190336 20010622
Priority number(s): FR19970007995 19970626

Also published as:
FR2765361 (A1)
US7036002 (B1)
TW457453 (B)
JP2000501541 (T)
HK1022756 (A1)
more >>

Abstract of **JP 2002055883 (A)**

PROBLEM TO BE SOLVED: To prevent unauthorized observation of an internal behavior of a processor by using a completely controlled standard circuit to enable simple diagnosis of design and failures by use of the conventional method. SOLUTION: This microprocessor includes a second work memory (52) and further includes a switching means to enable switch of use as the work memory to either one of two work memories (51, 52) as holding the contents of the two work memories (51, 52) during the implementation of a program and the switching means includes at least one register block (54) to store operation context of a program in a main memory and a switching circuit (53) to validate access registers (A1 to A3) (D1 to D3) to be connected with one work memory and the respective memories (51, 52, 6) and to be controlled by the switching circuit (53).



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－55883
（P2002－55883A）
(43)公開日　平成14年２月20日(2002.2.20)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ	５Ｂ０１７
15/78	５１０	15/78	５１０Ｇ	５Ｂ０６２

審査請求　未請求　請求項の数19　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－190336(P2001－190336)
(62)分割の表示　特願平11－505328の分割
(22)出願日　平成10年６月25日(1998.6.25)

(31)優先権主張番号　９７／０７９９５
(32)優先日　平成９年６月26日(1997.6.26)
(33)優先権主張国　フランス（ＦＲ）

(71)出願人　500268421
プル・セー・ペー・８
フランス国、エフ－78430・ルーブシエンヌ、ボワツト・ポスタル・45、ルート・ドウ・ベルサイユ、68
(72)発明者　ミシエル・ユゴン
フランス国、エフ－78310・モルパ、リユ・デ・セパージユ、６
(74)代理人　100062007
弁理士　川口　義雄

Ｆターム(参考)　5B017 AA03 BB04 CA13
5B062 DD10

(54)【発明の名称】　予測不可能なマイクロプロセッサまたはマイクロコンピュータ

(57)【要約】
【課題】　従来の方法の使用による単純な設計および障害の診断を可能にするために、完全に制御された標準の回路を使用して、プロセッサの内部挙動の不正な観察を防止する。
【解決手段】　第二の作業メモリ（５２）と、プログラム実行中に、その二つの作業メモリ（５１、５２）の内容を保持しながら作業メモリとしての使用をその二つの作業メモリ（５１、５２）のどちらか一方に切り替えることを可能にする切替手段とをさらに含み、この切替手段が、主メモリ中のプログラムの動作コンテキストを記憶する少なくとも一つのレジスタブロック（５４）と、一方の作業メモリおよび各メモリ（５１、５２、６）に結合されかつ切替回路（５３）によって制御されるアクセスレジスタ（Ａ１～Ａ３）（Ｄ１～Ｄ３）を妥当化する切替回路（５３）とを含む。

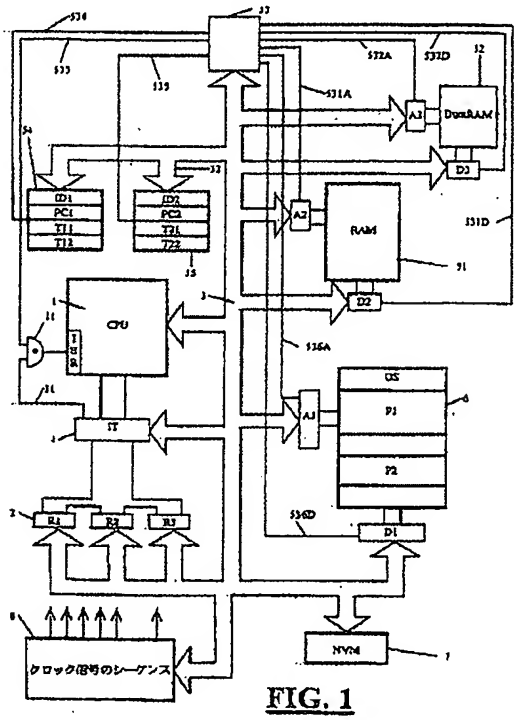


FIG. 1

【特許請求の範囲】

【請求項１】　プロセッサ（１）と、第一の作業メモリ（５１）と、オペレーティングシステムと主プログラム（Ｐ１）と二次プログラム（Ｐ２）とを含む主メモリ（６）と、第二の作業メモリ（５２）と、プログラムの実行中にその二つの作業メモリ（５１、５２）の内容を保持しながらその二つの作業メモリの一方の作業メモリから他方の作業メモリに切り替える切替手段と、各メモリ（６、５１、５２）に結合されたアクセスレジスタ（Ａ１～Ａ３）（Ｄ１～Ｄ３）とを有し、その切替手段が、主メモリ中のプログラムの動作コンテキストを記憶する少なくとも一つの第一のレジスタブロック（５４）と、一方の作業メモリと各メモリ（５１、５２、６）に結合されかつ切替回路（５３）によって制御されるアクセスレジスタ（Ａ１～Ａ３）（Ｄ１～Ｄ３）とを使用可能にする切替回路（５３）とを含む予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項２】　二次プログラムの動作コンテキストを記憶する第二のレジスタブロック（５５）をさらに含むことを特徴とする請求項１に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項３】　プログラムの実行を等時クロックから相関解除する手段（Ｒ１、Ｒ２、Ｒ３）をさらに含むことを特徴とする請求項１または請求項２に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項４】　作業メモリ（５１、５２）を切り替えかつ使用可能にする切替回路（５３）と、各作業メモリ（５１、５２）に結合されかつそれぞれ、主メモリ中のプログラムの動作コンテキストおよび二次プログラムの動作コンテキストを記憶する記憶レジスタブロック（５４、５５）とへロードすることによって、主プログラムが一つまたは複数の切替機構を使用可能にするかまたは抑止することができることを特徴とする請求項１から請求項３のいずれか一項に記載のマイクロプロセッサまたはマイクロコンピュータ。

【請求項５】　主プログラムによって利用される際に、作業メモリ（５１）およびそのアクセスレジスタ（Ａ２、Ｄ２）の代わりに第二の作業メモリ（５２）およびそのアクセスレジスタ（Ａ３、Ｄ３）が使用されることを特徴とする請求項１から請求項４のいずれか一項に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項６】　相関解除手段が、二次プログラム（Ｐ２）にランダムに飛び移ることによって、プロセッサ中のプログラムの実行を脱同期させるためにランダム割込みを、割込み回路（４）を介してトリガする乱数発生器（２）を含むことを特徴とする請求項３に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項７】　相関解除手段が、時間カウント後に、二次プログラムから主プログラムに復帰するために割込みをトリガする、プロセッサ（１）から独立した時間カウントシステム（Ｒ３）を含むことを特徴とする請求項４または請求項６に記載のマイクロプロセッサまたはマイクロコンピュータ。

【請求項８】　作業メモリを切り替える手段（５３、５４、５５、Ａ２、Ａ３、Ｄ２、Ｄ３）が、プロセッサおよびそのプログラムか、ランダム割込みシステム（２、４）か、タイマ（Ｒ３）か、またはこれら三つの要素のうちの少なくとも二つの要素の任意の組合せによって制御されることを特徴とする請求項４か請求項６か請求項７に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項９】　作業メモリを切り替える手段（５３、５４、５５、Ａ２、Ａ３、Ｄ２、Ｄ３）が、主プログラムのシーケンスを実行するプロセッサ（１）によってロードされることによって使用可能になることを特徴とする請求項１から請求項８のいずれか一項またはその組み合わせに記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１０】　第二のプログラム（Ｐ２）が主メモリ（６）中の主プログラム（Ｐ１）の作業領域と同じ作業領域を使用することを特徴とする請求項１から請求項９のいずれか一項に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１１】　第二のプログラム（Ｐ２）が主プログラムの作業領域より小さい作業領域を使用することを特徴とする請求項１から請求項９のいずれか一項に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１２】　切替手段が、マイクロプロセッサからの命令の実行サイクル中にメモリ（５１、５２、５３、５４、５５、Ａ２、Ａ３、Ｄ２、Ｄ３）およびそれに関連するコンテキストの置換を実行することを特徴とする請求項１から請求項１１のいずれか一項に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１３】　二次プログラム（Ｐ２）が主プログラム（Ｐ１）の一般動作コンテキストを修正せず、それによりこのコンテキストを回復する必要なしに主プログラムの復帰を可能にすることを特徴とする請求項１から請求項１２のいずれか一項に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１４】　主プログラム（Ｐ１）のコンテキストが、二次プログラム（Ｐ２）によって自動的に回復されるか、または制御権を主プログラム（Ｐ１）に戻す前に切替手段（５３）によって自動的に回復されることを特徴とする請求項１３に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１５】　主プログラム（Ｐ１）のメモリを二次

プログラム（Ｐ２）のメモリで置換する手段をさらに含むことを特徴とする請求項１から請求項１４のいずれか一項に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１６】　主プログラム（Ｐ１）が第一の作業メモリ（５１）および／または第二の作業メモリ（５２）を交互にまたは同時に使用することができることを特徴とする請求項１から請求項１５のいずれか一項に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１７】　切替回路（５３）へロードすることにより相関解除割込みのマスクまたはマスク解除が可能になることを特徴とする請求項４に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１８】　割込みをマスク解除するために、主プログラム（Ｐ１）または二次プログラム（Ｐ２）の命令を実行することによって、切替レジスタ（５３）が適切にロードされた後で二次プログラム（Ｐ２）によってトリガされる割込みによって主プログラム（Ｐ１）への復帰が実行されることを特徴とする請求項６に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【請求項１９】　モノリシック集積回路として実施されることを特徴とする請求項１に記載の予測不可能なマイクロプロセッサまたはマイクロコンピュータ。

【発明の詳細な説明】

【０００１】本発明は予測不可能なマイクロプロセッサまたはマイクロコンピュータに関する。

【０００２】マイクロプロセッサまたはマイクロコンピュータが、メモリに記録されたプログラムの過大な命令を、内部または外部からそのマイクロプロセッサまたはマイクロコンピュータに供給されたクロック信号の一つを基準とする一つまたは複数のタイミング信号に合わせて順次実行することは知られている事実である。

【０００３】このプログラム実行方法の様々な段階は時が経つにつれて精通できるようになることが分かっている。これは、命令の実行が、このプログラムによって予め決められたプロセスどおりに順序正しく行われ、一般にプロセッサを規則正しく調時するクロック信号と同期しているためである。実際に、すべてのプログラムは、予め分かっている順序で連続的に実行されなければならない命令シーケンスを生成し、また命令は時が経つにつれて所定のプロセスどおりに実行されるので、各命令が開始される瞬間および終了する瞬間は正確に知れる。したがって原理的には、実行されているプログラムは所定の命令シーケンスを含んでいるので、プロセッサの処理装置中で所与の瞬間に実行されている命令を知ることができる。

【０００４】例えば、プログラムまたは処理装置の始動時に実行される命令の数を決定したり、あるイベントすなわち外部または内部の基準信号から経過した時間、さらにはプロセッサのリセットから経過した時間を決定することができる。

【０００５】このようにマイクロプロセッサまたはマイクロコンピュータ中のプログラムの実行を観察できることは、このマイクロプロセッサまたはマイクロコンピュータが高度の機密保護を要する用途で使用されるときには大きな欠点となる。したがって、悪意のある人間がプロセッサの連続状態を調べ、この情報を使用して、内部処理に関するいくつかの機密の結果を入手することもできる。

【０００６】例えば、内部機密情報の試験、メッセージの暗号解読、さらには何らかの情報の完全性試験など、決められた機密保護操作の結果に応じて、様々な瞬間に所与の処置がとられることが想像できる。当該の瞬間に応じて、例えば、プロセッサに処置を施すか、または物理的調査によっていくつかのレジスタの値を得、それにより結果についての情報またはその情報の機密内容を得ることができ、さらには暗号計算の場合には使用された秘密暗号キーについての情報を得ることもできる。

【０００７】ランダムクロックパルスを発生させる回路を装備することによって機密保護マイクロコンピュータに初期の改善を施す装置がある。このようにすると、同期がすぐに実行不可能になるので、イベントを観察することで調査を実行することが特に困難になる。

【０００８】しかし、このタイプの解決策は多くの欠点を伴う。

【０００９】まず、マイクロコンピュータと同程度に複雑な回路全体にわたってランダム動作をシミュレートすることはできないので、このような回路の設計は特に巧妙かつ繊細になる。回路の挙動が乱雑なために製造終了時に回路を試験することはさらに困難である。実際に、クロックパルスのランダムシーケンスを回路の定義についてシミュレートすることは非常に困難であるが、特に内部バス上およびレジスタ中で信号が切り替わる期間中に全てのプロセッサの論理回路の全ての挙動を習得することはさらに困難である。

【００１０】これが本出願人による「ｉｍｐｒｏｖｅｄ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ、ｐｒｏｃｅｓｓ ｆｏｒ ｕｓｅ ｏｆ ｓｕｃｈ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ」と題する１９９６年３月７日のフランス特許Ｎ° ９６０２９０３の要求の主題である初期の改善がなされた理由であり、これによりプロセッサは定義期間中および試験期間中に通常の周期クロックで通常動作が可能になった。すなわち、プロセッサは保護モードと通常モードの間で切り替わることができる。機密保護を保証するために、パスワードまたは特別な暗号メッセージが入力されたときにのみそのプロセッサによってそのモードが活動化できることは容易に想像される。

5

【００１１】これらの難点に加えて、ランダムクロックの制御下で、すなわち全く無秩序な形で、シーケンス中に障害を診断するという難点がある。実際に、このような無秩序状態では、どうすれば問題を障害のある部分に限定することができ、またどうすれば問題が生じる正確な条件を決定することができるであろうか。

【００１２】ランダムクロックの使用は、理論上は興味深い改善策を与えるが、全く満足な解決策ではなく、とりわけ実際に実施することは容易でないことが分かる。

【００１３】本発明の一目的は、上述のタイプの調査を抑止する手段をプロセッサに装備すること、より一般的には、従来の方法の使用による単純な設計および障害の診断を可能にするために、完全に制御された標準の回路を使用して、プロセッサの内部挙動の不正な観察を防止することである。

【００１４】この目的は、プロセッサと、第一の作業メモリと、オペレーティングシステムと主プログラムと二次プログラムとを含む主メモリとを含む予測不可能なマイクロプロセッサまたはマイクロコンピュータが、

■第二の作業メモリと、

■プログラムの実行中に、その二つの作業メモリの内容を保持しながら作業メモリとしての使用をその二つの作業メモリの一方に切り替えることを可能にする通信手段とをさらに有し、

■この切替手段が、主メモリ中のプログラムの動作コンテキストを記憶する少なくとも一つのレジスタブロックと、一方の作業メモリと各メモリに結合されかつ切替回路によって制御されるアクセスレジスタとを妥当化する切替回路とを含むことを特徴とすることによって達成される。

【００１５】別の特徴によれば、この予測不可能なマイクロプロセッサまたはマイクロコンピュータは、二次プログラムの実行のコンテキストを記憶する第二のレジスタブロックを有する。

【００１６】別の特徴によれば、この予測不可能なマイクロプロセッサまたはマイクロコンピュータは、プログラムの実行を等時クロックに対して相関させる手段を有する。

【００１７】本発明の別の目的は、前記手段の実施がプロセッサ自体によって保証され、それにより上記手段によって与えられるいかなる追加の機密保護も、マイクロコンピュータ内にあり、したがって悪意のある処置に関して予測不可能であるオペレーティングシステムの決定のみに依存するようにすることである。

【００１８】この目的は、作業メモリ妥当化回路と各作業メモリに結合された記憶レジスタブロックとへロードすることによって、主プログラムが切替機構を使用可能にするかまたは抑止することができることによって達成される。

【００１９】別の特徴によれば、主プログラムによって

6

使用される際に、第一のメモリおよびそれ自体のアクセスレジスタの代わりに第二の作業メモリおよびそのアクセスレジスタが使用される。

【００２０】本発明の第三の目的は、クロック信号およびランダムタイミング信号を使用する必要なしに実行時間をプログラム自体から独立させることである。

【００２１】この目的は、相関解除手段が、二次プログラムにランダム接続することによってプロセッサ中のプログラムの実行を脱同期させるために割込み回路を介してランダム割込みをトリガすることができるランダム発生器を含むことによって達成される。

【００２２】別の特徴によれば、相関解除手段は、時間カウント後に、二次プログラムから主プログラムに復帰するために割込みをトリガする、プロセッサ１から独立した時間カウントシステムを含む。

【００２３】別の特徴によれば、作業メモリを切り替える手段は、プロセッサおよびそのプログラムか、ランダム割込みシステムか、時間カウンタか、またはこの三つのうちの少なくとも二つの組合せによって制御される。

【００２４】本発明の第四の目的は、レジスタの切替が機密情報への直接的または間接的なアクセスの手段と解釈されるのを防止することである。

【００２５】この目的は、作業メモリを切り替える手段が、主プログラムのシーケンスを実行しているプロセッサからの移行によって確立されることによって達成される。

【００２６】別の特徴によれば、第二のプログラムは、主メモリ中の主プログラムの作業領域と同じ作業領域を使用する。

【００２７】別の特徴によれば、第二のプログラムは、主プログラムの作業領域より小さい作業領域を使用する。

【００２８】別の特徴によれば、切替手段は、マイクロプロセッサの命令の実行サイクル中に作業メモリおよびそれに関連するコンテキストを置換する。

【００２９】別の特徴によれば、二次プログラムは主プログラムの一般動作コンテキストを修正せず、それによりこのコンテキストを回復する必要なしに主プログラムの復帰を可能にする。

【００３０】別の特徴によれば、主プログラムのコンテキストは、二次プログラムによって自動的に回復されるか、または制御権を主プログラムに戻す前に切替手段によって自動的に回復される。

【００３１】別の特徴によれば、この予測不可能なマイクロプロセッサまたはマイクロコンピュータは、主プログラムのメモリを二次プログラムのメモリで置換する手段を含む。

【００３２】別の特徴によれば、主プログラムは、第一の作業メモリおよび／または第二の作業メモリを交互にまたは同時に使用することができる。

【００３３】別の特徴によれば、切替回路へロードすることにより相関解除割込みのマスクまたはマスク解除が可能になる。

【００３４】別の特徴によれば、割込みをマスク解除するために主プログラムまたは二次プログラムの命令を実行することによって切替レジスタが適切にロードされた後で主プログラムへの復帰が二次プログラムによってトリガされた割込みによって実行される。

【００３５】別の特徴によれば、この予測不可能なマイクロプロセッサまたはマイクロコンピュータはモノリシック集積回路からなる。

【００３６】本発明の他の特徴および利点は、添付の図面を参照しながら以下の説明を読めばより明らかになろう。

【００３７】図１は、本発明の一実施形態による集積回路の電子図である。

【００３８】図２は、割込みの出現およびマスク解除された割込みの確認に関する命令の実行のタイミング図である。

【００３９】図３は、一つの集積回路の記憶レジスタのロード回路の代替設計を示す図である。

【００４０】図４は、回路の通常動作への復帰を可能にするプログラム部分（Ｐ２）を示す論理図である。

【００４１】図１に本発明の一実施形態を示す。ＳＵＭＩＣ（Ｓｅｌｆ－Ｕｎｐｒｅｄｉｃｔａｂｌｅ　ＭＩＣｒｏｃｏｍｐｕｔｅｒ）と呼ばれる、本発明が包含するマイクロプロセッサまたはマイクロコンピュータは、処理装置（１）と、実行すべきプログラムを含む不揮発性メモリ（６）と、そのアドレスレジスタ（Ａ２）およびそのデータレジスタ（Ｄ２）を備えたＲＡＭ（５１）と、例えば規則的かつ予測不可能な瞬間にパルスを供給するランダムまたは疑似ランダム信号発生器（２）と、割込み回路（４）と、レジスタ回路（Ｒ２）と、タイマ（Ｒ３）と、シーケンサ回路（８）と、不揮発性メモリ（７）（ＮＶＭ）と、そのアドレスレジスタ（Ａ３）およびそのデータレジスタ（Ｄ３）を備えた揮発性タイプのダミーメモリ（ＤｕｍＲＡＭ）（５２）と、通常動作に復帰するためのパラメータを記憶する二つのレジスタスタック（５４、５５）と、例えばアドレスレジスタ（Ａ１）および（Ａ３）、データレジスタ（Ｄ１）および（Ｄ３）、第一の記憶レジスタブロック（５４）および第二の記憶レジスタブロック（５５）の動作を検査するのに十分な数のセルを有するレジスタを含む切替回路（５３）とを備えたモノリシック集積回路を含む。この切替レジスタ（５３）はバス（３）を介して処理装置（１）によってロードされる。この切替レジスタ（５３）の状態は、より詳細には、プロセッサの作業メモリ領域内またはこの領域外のＲＡＭおよび／またはＤｕｍＲＡＭを妥当化するために使用される。

【００４２】このモノリシック集積回路では、処理装置はバス（３）によって様々なメモリに接続され、各メモリはそれぞれアドレス（Ａ１、Ａ２、Ａ３）を有するレジスタとデータレジスタ（Ｄ１、Ｄ２、Ｄ３）とに向かって進み、各アドレスレジスタおよびデータレジスタはそれぞれ切替回路（５３）からきたコマンド線（５３１Ａ、５３２Ａ、５３６Ａ）、（５３１Ｄ、５３２Ｄ、５３６Ｄ）によってそれぞれロックすることができる。この切替回路はまた他の三つのコマンド線を含み、そのうちの一つ（５３３）は、二つの入力を有するＡＮＤゲートで終端し、そのうちの第二の入力は割込み回路からきたバス線（３１）を受ける。このＡＮＤゲートの出力は、割り込みイネーブルレジスタ（ＩＥＲ）ビットの一つに直接接続され、これにより切替回路が活動化されていないとき、したがって線（５３３）が活動状態でないときのみ、割込み回路（４）によってトリガされた割込みをマスクする。

【００４３】他の二つの線（５３４、５３５）はそれぞれ、記憶レジスタの二つのブロックまたはスタック（５４、５５）の一方をロックする。これらのブロックはそれぞれ、以下に述べる情報を記憶するためのいくつかの記憶レジスタ（５４）および（５５）を有する。これらのレジスタ（５４、５５）は、各メモリに共通のバス（３）に接続される。このバス（３）は、制御線（５３１Ａ、５３２Ａ、５３２Ｄ、５３６Ａ、５３６Ｄ、５３３、５３４、５３５）を所望の動作モードに応じて活動状態または非活動状態にするのに必要な値を切替回路（５３）にロードするために使用される。不揮発性メモリ（６）は、回路オペレーティングシステムと、以下主プログラムと呼ぶ第一のアプリケーションプログラム（Ｐ１）と、以下二次プログラムと呼ぶ第二のプログラム（Ｐ２）とを含み、またシーケンサ（８）と、レジスタ（Ｒ２）と、タイマ（Ｒ３）と、ランダム発生器（Ｒ１）とがバス（３）に接続され、これら三つの要素（Ｒ１、Ｒ２、Ｒ３）は、プロセッサの割り込みイネーブルレジスタ（ＩＥＲ）を使用して、プロセッサの割込み入力（１）に接続された割込み発生器回路（４）に接続される。ＩＥＲのビットの一つは一般に、一部のユーザに固有の用途のために取っておかれ、使用可能になっている。

【００４４】第一の実施形態では、不揮発性メモリ（６）に含まれた主プログラム（Ｐ１）は、必要に応じてバス（３）を介して切替回路（５３）の状態を修正するが、このプロセスは実行に関して何らの難点も示さない。これにより直ちに、ＣＥ（Ｃｈｉｐ　Ｅｎａｂｌｅ）入力に作用して、メモリパッケージと第一のブロック（５４）を通常動作に復帰させるのに必要な全てのレジスタとを妥当化することによって主作業ＲＡＭ（５１）またはこのメモリの一部分が切り替わる。これらのメモリおよびレジスタはスタティックタイプにし、それによりそれらを維持するために必要なエネルギーを節約

できることが有利である。したがって、切替回路（５３）は主作業メモリ（５１）をダミーメモリ（５２）で置換し、それにより主作業メモリの代わりに専らダミーメモリを使用してプログラムが実行されるようにする。このダミーメモリ（５２）は、それが置換されたメモリと同じアドレスにあることもあるが、異なるアドレスにあることもある。一つの有利かつ経済的な解決策は、このダミーメモリとして非常に小さいＲＡＭを使用することである。実際に、このダミーメモリは主プログラムの機能上の役割を果たすものではなく、アドレス可能領域はアドレスレジスタ（Ａ３）の長さを短縮するだけで制限できる。また、いくつかのアドレスレジスタブロック間で排他的ＯＲをとることによってアドレスをそれ自体に「折り返す」こともできる。したがって、主作業メモリのアドレス可能領域が５１２バイトである場合、ダミーメモリは容易に３２バイトに制限でき、したがって非常に経済的な解決策が得られる。３２バイトは、例えば、単に主作業メモリのマトリックスにＲＡＭメモリ線を追加した場合に対応する。この場合、この線はそれ自体のアドレスレジスタ（Ａ３）および障害レジスタ（Ｄ３）を有することになる。切替回路（５３）は、ダミーメモリを活動化したとき、ＮＶＭへの書込みアクセスを抑止し、それによりその内容が乱されることがないようにすることもできる。

【００４５】切替を実行するためには、二つのレジスタのブロック、すなわち第一のブロック（５４）と第二のブロック（５５）を交互に使用することが有利な場合があり、各ブロックは、プログラムを実行するために必要なコンテキスト全体、より具体的に言えば、第一のブロック（５４）用のプログラムカウンタ（ＰＣ１）、第二のブロック（５５）用のプログラムカウンタ（ＰＣ２）、第一のブロック用の命令復号レジスタ（Ｄ１）、第二のブロック用の命令復号レジスタ（Ｄ２）、および（Ｔ１１、Ｔ１２、およびＴ２１、Ｔ２２）で表される他のレジスタを含む。このレジスタ（Ｔ１１、Ｔ１２、Ｔ２１、およびＴ２２）は、例えば使用するマシンサイクル数など、同じ動作パラメータを保持する。これら全てのレジスタは切替回路（５３）によって自動的に切り替えられる。アドレスの変更は、この場合、特定の命令を使用してプログラムカウンタの内容をレジスタスタック中に保存するために、大抵のマイクロ計算機の場合と同様に何らの負担もなしに直ちに実行される。したがって、両方向の切替は非常に迅速であり（一般にクロックサイクルよりはるかに短い）、したがってこの装置の機密保護レベルはかなり高くなる。同じ機構は、（Ｔ１１～Ｔ２２）など、プロセッサの動作コンテキストを保存するその他のレジスタにも使用できる。

【００４６】プログラム（Ｐ１）が切替レジスタをロードすることによってダミーモードの集積回路を活動化したとき、切替回路（５３）は、ダミー回路の動作の前にパラメータを保持する第一のレジスタスタック（５４）を抑止して、プログラム（Ｐ１）が中断されている場合にその第一のレジスタスタック（５４）を再開することを理解されたい。一方、第二のレジスタスタック（５５）は、プログラム（Ｐ２）を実行するために同じダミーメモリを有する回路の通常動作を使用可能にするために使用されることになる。また、この場合、ダミーモードでの動作に対応する割込みマスクＩＥＲレジスタビットはマスク解除され、それによりランダム発生器によってかまたは前にランダム発生器によって乱数をロードされたタイマ（Ｒ３）によって割込みが生成される間に、またこの乱数によってかまたは特定の情報をロードされたレジスタ（Ｒ２）によって表された時間の実行が終了した時に使用可能になり、割込みがトリガされ、（３１）プログラム（Ｐ１）の制御下の通常動作からプログラム（Ｐ２）の制御下のダミーモードでの動作への切換が起こることは明らかである。

【００４７】図２に割込みモードでの動作を示す。この図には、割込み回路から線（３１）上を処理装置（１）に向かって伝送される第一の割込みパルスＩＴは、レジスタによってマスクされたために考慮されておらず、この割込みのマスクは、命令「ＭＯＶＥ　ｉｍｍｅｄｉａｔｅ　ｄａｔａ　ｔｏ　ｒｅｇｉｓｔｅｒ　ＩＥＲ（隣接するデータをレジスタＩＥＲに移動せよ）」を使用し、それによりそのデータをマスクするレジスタにロードすることが示されている。現在の命令は分岐割込みをマスク解除すると仮定する（ただしこれは異なる時刻で他の命令によって実行できる）。この場合、第二のパルスは処理装置（１）によって考慮され、その結果切替回路（５３）が切り替わり、したがって第二のレジスタブロック（５５）およびＤｕｍＲＡＭ（５２）が第一のブロック（５４）およびＲＡＭダミーメモリ（５１）の代わりに活動状態になる。割込みの確認は、ある状態から別の状態に遷移する間、例えば（Ｓ２）と（Ｓ３）の間にのみ可能であり、それによりマシンの安定かつ一貫した状態を記憶し、とりわけ中断されたプログラムが復帰するときと全く同じ状態を回復することに留意されたい。この割込みが確認された場合、通常の場合と同様に命令の終了時に、中断されたプログラムが回復されたとき、これは通常次の命令で行われるので特に問題は生じない。逆に、割込みは命令の実行中、例えば状態（Ｓ２）で発生した場合、順序づけ回路を同様に回復させ、それにより中断されたプログラムの回復時に状態（Ｓ３）を正しくトリガする必要があることは明らかである。これは、例えば、回復の瞬間にバス（３）を介してレジスタ（Ｔ１１）とシーケンサ（８）との間の直接リンクによって達成できる。このリンクは、バス（３）を介さずに特定のものにすることもできる。また、シーケンサ自体に状態記憶レジスタを含めて、この段階中のバスの移動を防止することが有利なこともある。

【００４８】このように、割込みを用いて、主プログラム（Ｐ１）は以下に述べるように二次プログラム（Ｐ２）を使用可能にすること、および／または二次プログラム（Ｐ２）に切り替わることができる。二次プログラムが活動状態でなくなったとき、切替回路（５３）の状態は変化し、ＲＡＭ作業メモリは何らの修正もなしにその最初の構成を回復し、その結果主プログラムは、正確にそれが中断された時点でその経路を回復することができる。また、主プログラム（Ｐ１）は、保護が必要なときには、それ自体が二次プログラム（Ｐ２）に分岐することにより、最初にまたは処理中にそれが選択した瞬間に作動してランダム長さを生成し、それにより様々なシーケンスをスクランブルするような形で実行することもできる。その場合、このプロセスの動作は、例えばその時間の長さが発生器（２）から得られた乱数に依存する待機ループをトリガすることができる二次プログラム（Ｐ２）によって制御することができる。二次プログラムは、二次プログラムが新しい制御権を主プログラムに移すとすぐに、さらには次の割込み時に、主プログラムがその通常のプロセスを再開できるように主プログラムが使用していないメモリの一部分を使用して、または前と同様にタイマを使用して、またはこの二つを組み合わせて使用して実行することができる。二次プログラムはまた、制御権を主プログラムに移す前に主プログラムのコンテキストを回復する限り、共用資源を使用することもできる。

【００４９】これらの機構は、二次プログラムの実行の終了時に復帰を伴う主プログラムの二次プログラムへの分岐の実行に類似するが、本発明の機構は以下の点で特に異なることを述べておきたい。

【００５０】■二次プログラムは、主プログラムに必ず関係するいかなる機能も実行しない。

【００５１】■ダミーメモリ（５２）のサイズは、プログラムの通常の実行に必要とされるよりはるかに小さくすることができる。

【００５２】■ダミーメモリ（５２）の内容は単にトラックをカバーするだけなので重要ではない。

【００５３】■この高速機構を用いれば、二次プログラムの命令を主プログラムの命令と組み合わせることができる。

【００５４】■二次プログラムの内容は単にトラックをカバーするために使用されるだけなので保存する必要はない。

【００５５】第二の実施形態では、プロセッサは、回路（５３）を切り替えたとき、同時にランダム発生器（２）によって、または不揮発性メモリＮＶＭ（７）の内容から初期化されるタイマ（Ｒ３）を活動化する。例えばＥ２ＰＲＯＭタイプのＮＶＭまたは強誘電性装置は、実際に、ＮＶＭが使用されるたびに修正される単一の数を含むことができる。タイマ（Ｒ３）は、予測不可能な時間期間後に満了したとき、主プログラムへの復帰をトリガし、また切替回路（５３）を切り替えて、主メモリを作業領域に戻す。この機構は、従来の割込みによるか、または切替回路（５３）へのタイマ（Ｒ３）の直接作用およびレジスタ（ＰＣ１）および（ＰＣ２）への作用により実行され、それにより（ＰＣ１）や（ＰＣ２）など処理装置（１）によるプログラムの実行を検査することができる。

【００５６】代替実施形態では、ランダムに選択されたアドレスを最初に指し、次いでそのアドレスから得られたバイトを反転させ、かつ／または例えば逆配線によるかまたはアドレスの内容のための左シフト回路によってレジスタ（ＩＤ２）の内容を反転させる、主プログラム（Ｐ１）の任意の部分を二次プログラム（Ｐ２）として使用することができる。このようにすると、プログラムが全く異なる命令を実行するようにすることもできる。

【００５７】異なる命令を実行する別の代替形態は、図３に示されるようなものである。レジスタ復号一時命令ＩＤＴは、一方ではバス（３３）の一部分によってバス（３）に接続され、他方ではバス（３４）の一部分によって回路状態の記憶を可能にする第二のレジスタスタック（５５）に接続される。バス（３４）の一部分は、レジスタＩＤＴのビット（Ｂ７）をレジスタ（ＩＤ２）のビット（Ｂ４）に、レジスタＩＤＴのビット（Ｂ６）をレジスタ（ＩＤ２）のビット（Ｂ１）に、レジスタＩＤＴのビット（Ｂ５）をレジスタ（ＩＤ２）のビット（Ｂ３）に接続する特定の配線によってスタック（５５）のレジスタ（ＩＤ２）にハードウェアによって接続される。

【００５８】最後に、最後の代替形態は、全く異なる（命令の）実行を可能にし、またバス（３）がバス（３５）の一部分によってＩＤＴ一時命令復号レジスタに接続された図３に示す実施形態を含む。このバスの別の部分（３７）は、このＩＤＴレジスタを、いくつかの入力を有する排他的ＯＲゲート（３９）に接続する。このＯＲゲートの他の入力は、バスの一部分（３６）をロードされてバス（３）に関連づけられるレジスタ（Ｒ’２）にバス（３８）によって接続される。このレジスタ（Ｒ’２）には、「ＭＯＶＥ　ｒｅｇｉｓｔｅｒ（Ｒ１）（for instance）ｔｏ　ｒｅｇｉｓｔｅｒ（Ｒ’２）（レジスタ（Ｒ１）を（例えば）レジスタＲ‘２）に移動せよ）」などの命令によって、ランダム発生器（Ｒ１）かタイマか不揮発性メモリＮＶＭ（７）から得られるものなど、任意の情報をロードすることができる。このタイプのシフト命令はマイクロプロセッサの分野の当業者にはよく知られており、実施に関して何らの困難も伴わない。レジスタ（Ｒ’２）からの情報とＩＤＴレジスタにロードされた値との排他的ＯＲをとることは、プログラム命令（Ｐ２）を全く変更し、したがって全く異なる命令を実行する一つの方法である。

【００５９】プログラム（Ｐ２）中では、ランダムな形で呼び出されることになる多数のシーケンスを使用することができ、各シーケンスは、様々な命令の組を実施することになり、これには各分岐ごとに異なる処理時間および様々なマイクロプロセッサ挙動を伴う。シーケンスは、例えば主プログラムが二次プログラムに飛び移った後でランダムに呼び出すことができ、この二次プログラムは、メモリ（７）からのランダム値Ｖを二つのレジスタ、例えばマイクロプロセッサ（１）の（Ｔ.2.1）および（Ｔ２２）にロードする。二次プログラムはこの値Ｖを増分し、次いでこのプログラムは増分したこの値を不揮発性メモリ（７）に記憶するよう命令する。不揮発性メモリ（７）に記憶されたこの値は、後で使用できるようになされている。二次プログラムは、次いで（Ｔ２１）中のｎ個のＭＳＢまたはＬＳＢをサンプリングして、様々な二次プログラムシーケンスの中から実行すべきプログラムシーケンスを選定することを可能にする値ｒを得る。

【００６０】第三の実施形態では、プロセッサ（１）は、ランダム発生器（２）の状態を調べるための読取り命令によるか、所定のパルスを直接読み取るか、それらのいくつかをグループ化するか、さらにはランダム発生器（２）によってロードされたレジスタ（Ｒ２）の内容を考慮することによりランダム発生器（２）に問い合わせることができる。主プログラムは、保護が必要なときには、前述の機構と同様にして制御権を二次プログラムに移す。

【００６１】当然、前述の実施形態の効果は、一方ではランダムクロックを備えることにより、他方では主プログラム自体か、または主プログラムが許可するかまたは許可しないランダム割込みシステムによって主プログラムの実行を中断できるようにすることにより組み合わせることができる。

【００６２】また、主プログラムの実行は、ランダム発生器かプログラムかタイマか二次プログラムに依存するか、または一度に二つ、三つ、四つの要素に依存する絶対に予測不可能な順序づけに従って達成されることが明らかである。主プログラムはまた、機密保護の観点からは機密でない機能を実行するときには通常動作に頼り、それにより例えば結果を外界に供給するか、タイマ（Ｒ３）またはランダム発生器（２）の相関解除割込みをマスクし、それにより処理時間を最適化することができる。機密保護機能が実施されるとすぐに、主プログラム（Ｐ１）は、相関解除割込みを妥当化し、それによりランダムモードでの動作を「スクランブル」することによってその動作を可能にする。

【００６３】同じく図１に示す第四の実施形態によれば、ＲＡＭ（５１）および（５２）を同時に使用することができる。実際に、メモリおよびそれに関連するレジスタの切替を検出することができると仮定した場合、ダミーメモリ（５２）を使用してシーケンスを除去することによって分析を実行できる場合もある。このような万一の場合を回避するために、この実施形態では、第一の段階中にメモリ（５１）および（５２）を並列に妥当化できるようになされている。明らかに、このことは、メモリ（５２）がこの場合少なくともプログラム（Ｐ１）と共に動作しているメモリ（５１）中の、プログラム（Ｐ１）によって使用される領域のサイズに等しいサイズを有することを前提条件とする。このようにして、それぞれメモリ（５１）および（５２）中の、プログラム（Ｐ１）によって使用される二つのメモリ領域の内容は、この第一の段階中にこのプログラムによって同様にして初期化され、使用される。一つの代替形態は、読取りサイクル中に必要な構成を有する切替回路（５３）に二つのレジスタの一方（Ｄ２）または（Ｄ３）のみをロードして競合を防止することによって妥当化を行うことであるが、これは本発明に根本的な変更を加えるものではない。したがって、この段階中に実際に使用されているメモリを識別することはできない。したがって、第二の段階中に、切替回路（５３）に修正を加えることによってメモリを交互にかつランダムに切り替え、同時に同じプログラム（Ｐ１）を実行し続けることが可能になる。したがって、あるプログラムまたは別のプログラムの実行をＲＡＭまたは使用されているレジスタに相関させることはもはや不可能になる。第三の段階では、前述のように予測不可能な瞬間にプログラム（Ｐ２）を介してダミーメモリ（５２）を切り替え、同時に主作業メモリ（５１）への復帰も予測不可能な瞬間に行う。このプロセスは、保護措置として主プログラム（Ｐ１）の制御下で任意に再現可能である。

【００６４】最後に、本発明が提供する最後のプログラムは、プログラム（Ｐ２）のダミーモードから出て、プログラム（Ｐ１）を伴う通常動作モードに復帰することができるプログラムである。プログラム（Ｐ１）は、制御権をプログラム（Ｐ２）に移す直前に、ランダム発生器からかまたはタイマから来る割込みを使用可能にし、同時にそれを初期化する。無秩序プログラム（Ｐ２）の実行中に、回路（４）を介した割込みが発生し、これは割込みプログラム（ＰＩＴ）に移る。このプログラムは、通常割込みベクトルを用いてアクセスされ、例えば現在のプログラムの実行コンテキストを分析する。（Ｐ２）が活動状態の場合、ＰＩＴは制御権をプログラム（Ｐ１）に移す。この機構は、以下のように実行できる。ＰＩＴプログラムの第一の命令が実行されたとき、これは例えば図４に示すように、切替回路（５３）の内容を読み取り（４１）、次いで回路（５３）に含まれる情報がダミーモード動作に対応するかどうかを決定する試験を行う（４２）ことによって構成できる。肯定の場合、ＰＩＴプログラムは、ステップ（４３）で表されるプログラム復帰命令（Ｐ１）を実行する。この復帰は、

線（５３４）および（５３１）の値を修正することステップ（４４）に従って切替レジスタ（５３）の書込みを行うことによって開始される。切替レジスタ（５３）へのこの後続の書込み（４４）により、線（５３４）および線（５３１）の値の修正された通常モードに復帰し、それにより再度スタック（５４）および主作業メモリ（５１）の使用を許可することができる。プログラム（Ｐ１）への復帰のこの命令は、ダミー試験（４２）の直後か、またはランダム時間の生成を可能にする表されていない他のいくつかの命令の実行の直後に実行することができる。試験（４２）が否定の場合、プログラムはステップ（４５）に進み、ダミーモードに変更するよう切替レジスタ（５３）への書き込みを行い、それにより線（５３５）および（５３２）の値を修正して、（５３１）および（５３４）の制御下で回路をロックしながらレジスタスタック（５５）およびダミーメモリの使用を可能にする。

【００６５】前記の全ての実施形態で、ランダムクロックを使用する必要はないことに気づくであろう。逆に、クロック配分を全く通常の等時配分にして、回路の設計ならびにそのシミュレーションおよび試験を容易にすることができる。実際に、機密保護は、もはやプロセッサがランダムに調時されることによって与えられるのではなく、これらのプログラムが等時クロックに合わせて、またはこれに合わせずにそれなりに実行され、実行自体がスクランブルされることによって与えられる。

【００６６】プロセッサが実行するプログラムの編成は、マシンが実行するプログラムのタイプに従って実施される妨害のタイプを決定する実際の機密保護オペレーションシステムによって、プロセッサの動作が制御されるように実施することができる。この場合、オペレーティングシステムは、ランダム発生器からきた様々な信号、割込み、主プログラムおよび二次プログラムの起動を適宜に管理する。明らかに、二次プログラムは、単純な待機ループ以外の機能、特に二次プログラムに与えられた時間を利用するために主プログラムにとって有効である処理を実行するために使用できる。この処理は、例えば主プログラムが後で使用する予備計算を含む。当然、プロセッサがマルチアプリケーションモードで動作し、同時にアプリケーションプログラムが単純な主プログラムと見なせるときには、本発明の機構は容易に一般化できる。

【００６７】上述のランダム発生器およびタイマは、製造に関して特に何らの問題も生じず、また本発明と何らの関係もない他の用途に別々に使用するときに当業者に知られている。

【００６８】ランダム発生器に関しては、例えば、様々な周期を有するループカウンタを使用することができる。これらのカウンタは、不揮発性メモリ（７）に記憶された初期化情報によって初期化される。プロセッサが始動したとき、カウンタは初期値として記憶された値を考慮する。計算中またはその終了時に、不揮発性メモリは、次の初期化時にカウンタを初期化するために初期化情報として使用される新しい値で更新される。上述の割込みパルスの生成は、生成された数がプログラムデータの一部と等しいなどの特徴を有するときに行われる。また、一つまたは複数のカウンタの一つまたは複数のビットの値を使用することもできる。また、暗号アルゴリズムかまたは上述の初期化情報によって初期化されたチョッピング機能を使用して、非常に良好なランダム発生器を得ることもできる。この場合、発生器は、このアルゴリズムを実施するプログラムにすることができる。この乱数発生器は上述の様々な乱数を発生させるためにも使用できることは明らかである。このような発生器を得る別の方法は、「ノイズダイオード」の両端子間で発生した電圧を増幅し、低域フィルタを通過させた後で信号を整形して、過度に高速なノイズパルスがマイクロプロセッサの動作を妨害しないようにすることである。

【図面の簡単な説明】

【図１】本発明の一実施形態による集積回路の電子図である。

【図２】割込みの出現およびマスク解除された割込みの確認に関する命令の実行のタイミング図である。

【図３】一つの集積回路の記憶レジスタのロード回路の代替設計を示す図である。

【図４】回路の通常動作への復帰を可能にするプログラム部分（Ｐ２）を示す論理図である。

【図１】

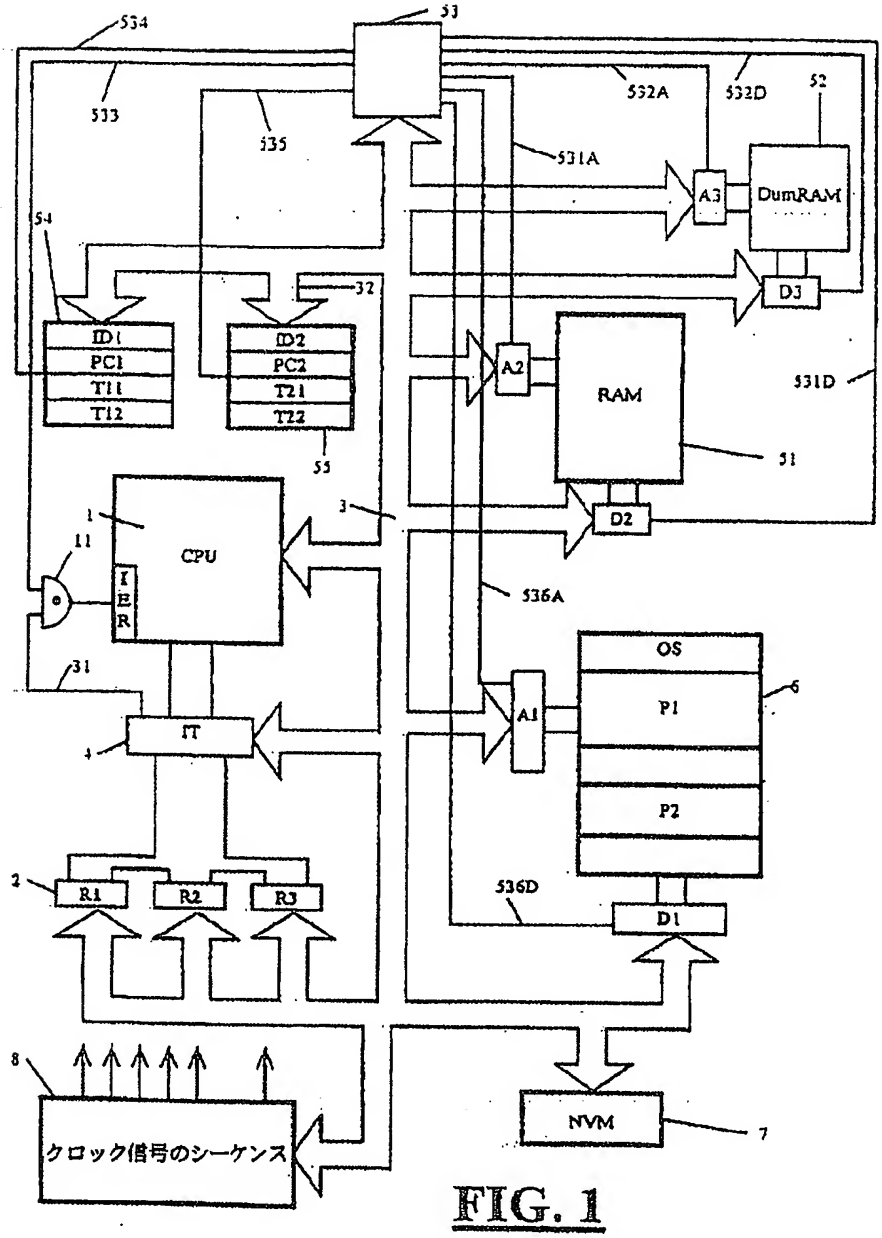


FIG. 1

【図２】

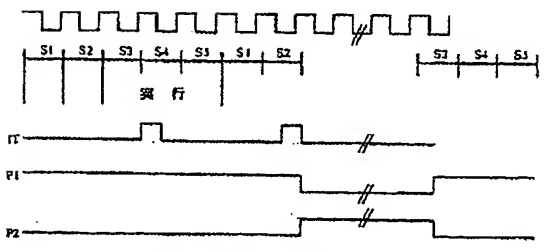


FIG. 2

【図３】

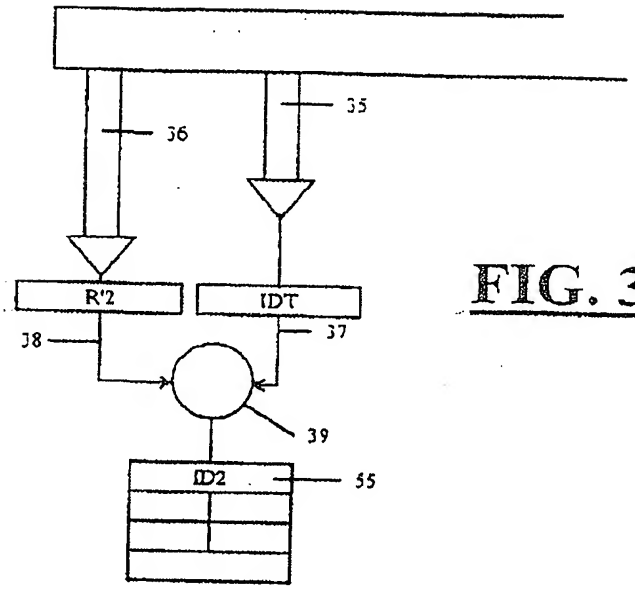


FIG. 3B

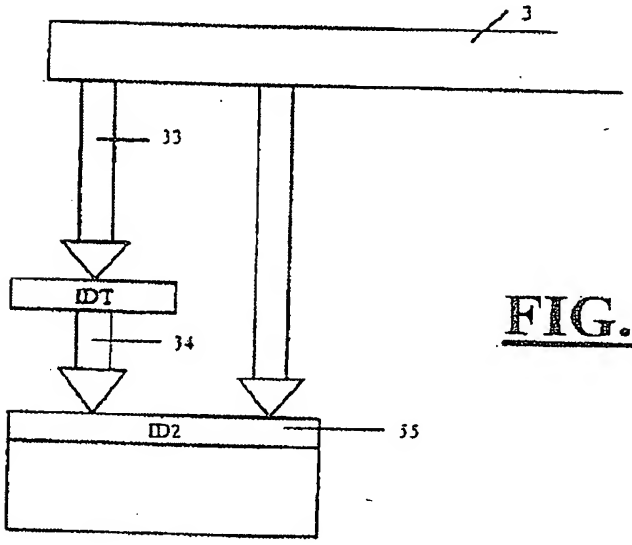


FIG. 3A

【図４】

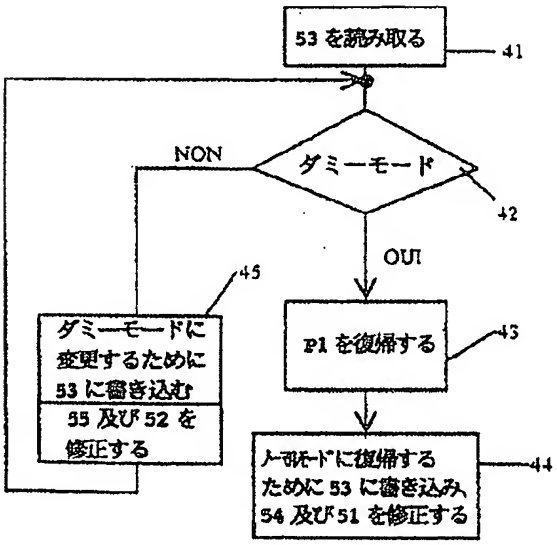

53 を読み取る
41
NON
ダミーモード
42
OUI
45
ダミーモードに
変更するために
53 に書き込む
55 及び 52 を
修正する
P1 を復帰する
43
ノーマルモードに復帰する
ために 53 に書き込み、
54 及び 51 を修正する
44

FIG. 4